IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

REMEDPAR, INC.,	**)**	
	)	
Plaintiff,	**)**	
	)	
v.	**)**	**Civil Action No. 3:09-cv-00807**
	)	
ALLPARTS MEDICAL, LLC and **THOMAS CAMACHO,**	**)** **)**	**Judge Thomas A. Wiseman, Jr.**
	)	
Defendants.	**)**	

MEMORANDUM OPINION

In this action, plaintiff ReMedPar, Inc. ("RMP") has filed a Verified Complaint asserting federal claims against defendants AllParts Medical, LLC and Thomas Camacho (collectively, "Defendants") for violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, as well as supplemental state-law claims based upon violation of the Tennessee Uniform Trade Secrets Act and the Tennessee Personal and Commercial Computer Act. In a nutshell, RMP alleges that that Defendants "[stole] the intellectual property of ReMedPar and exploit[ed] it to unfairly compete with ReMedPar" (Doc. No. 1, Verified Compl. at 1), as a result of which RMP seeks damages as well as declaratory and injunctive relief. This Court's original jurisdiction is premised upon the federal claims arising under the CFAA, with supplemental jurisdiction over the state-law claims pursuant to 28 U.S.C. § 1367(a).

Defendants have now filed separate Motions to Dismiss (Doc. Nos. 31 and 33) in which they seek dismissal of the Verified Complaint on the grounds that RMP has failed to assert a claim under the CFAA, and that the Court, after dismissing RMP's federal claims, should decline to exercise supplemental jurisdiction over the remaining state-law causes of action.

I. STANDARD OF REVIEW

A motion under Rule 12(b)(6) of the Federal Rules of Civil Procedure seeks to have the complaint dismissed based upon the plaintiff's failure to state a claim upon which relief can be granted. The reviewing court must "accept all the . . . factual allegations as true and construe the complaint in the light most favorable to the Plaintiff[ ]." *Gunasekera v. Irwin*, 551 F.3d 461, 466 (6th Cir. 2009) (citation and internal quotation marks omitted). "To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain either direct or inferential allegations respecting all the material elements to sustain a recovery under some viable legal theory." *Advocacy Org. for Patients & Providers v. Auto Club Ins. Ass'n*, 176 F.3d 315, 319 (6th Cir. 1999) (internal quotation marks omitted). "[E]ven though a complaint need not contain 'detailed' factual allegations, its 'factual allegations must be enough to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true.' " *Ass'n of Cleveland Fire Fighters v. City of Cleveland*, 502 F.3d 545, 548 (6th Cir. 2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

II. FACTUAL ALLEGATIONS

According to the allegations in plaintiff RMP's Verified Complaint, which the Court accepts as true for purposes of Defendants' motions, RMP is a Delaware corporation whose principal place of business is in Goodlettsville, Tennessee. RMP specializes in the sale of after-market medical diagnostic imaging equipment and replacement parts, and in providing technical support, technical repair and training services. Defendant AllParts is a Tennessee limited liability company that is also engaged in the sale of after-market medical imaging equipment and replacement parts and is RMP's direct competitor. Defendant Camacho, a Tennessee resident, was employed by RMP from April 15, 2002 through September 8, 2008, the vast majority of which time he served as RMP's Director of Information Technology. At some point in 2009, Camacho apparently began working for AllParts. Several of RMP's former employees had left RMP to found AllParts in 2006. Since then, a number of other former RMP employees besides Camacho have been induced to leave RMP to go to work for AllParts.

RMP uses a computer application it calls "ROCS," which is RMP's proprietary Enterprise Resources Planning ("ERP") and Customer Relations Management ("CRM") platform through which RMP utilizes electronic data and software to operate its business. The ROCS application serves as RMP's core inventory, purchasing and customer information database. On the CRM side, ROCS contains all of RMP's customer information, including contact information, purchase history, prices paid in prior transactions, as well as specific account notes about each customer. On the ERP side, ROCS contains an extensive library of information on approximately 20,000 parts that has been compiled by RMP over the years.

RMP developed ROCS specifically for its own use, and the platform cannot be purchased by other companies in the market. RMP has used the application to compile a vast amount of proprietary and confidential information. RMP has engaged in and continues to engage in substantial efforts to maintain the secrecy of its confidential and proprietary information, including ROCS and the information compiled through the use of ROCS, and to prevent dissemination of its confidential information in the marketplace. RMP has never given permission, through a license agreement or otherwise, for AllParts or any other company to use ROCS. RMP disseminates a Policy and Procedures Manual to its employees, who are required to sign receipts acknowledging that they have read, understood and agree to abide by its provisions. Included in the Policy and Procedures Manual is an express Confidentiality Policy.

In August 2009, RMP interviewed a person who was then employed by AllParts for a Customer Service Representative position with RMP. Through that person, RMP learned that AllParts had been using an early version of ROCS since at least 2007. RMP also learned that in July 2009, AllParts' computer system underwent a substantial upgrade and that, after the enhancement, the version of ROCS used by AllParts acquired the same screen appearance and layouts as RMP's current version of ROCS. After the upgrade, the functionality of the AllParts system was virtually identical to ROCS. RMP also learned that, beginning in January 2009, Thomas Camacho, a former RMP employee, was frequently at AllParts' business location, and frequently in contact with Scott Young, AllParts' shipping manager, and with Wanda Legate, AllParts' Vice President of Customer Relations and also a founder and principal of AllParts. Both Young and Legate are former RMP employees, and both knew or should have known the confidential nature of RMP's ROCS application and the information compiled and stored through the use of ROCS. The purpose of Camacho's work at AllParts was to maintain and upgrade the software that operates AllParts' computer system. Camacho was engaged as an independent contractor to implement enhancements to AllParts' computer system, which he in fact did.

While he was still employed by RMP, Camacho was responsible for the maintenance, modification and enhancement of ROCS. Camacho had access to and created upgrades to the source code for ROCS and was responsible for integrating ROCS into RMP's computer system. He was responsible for maintaining and providing support for RMP's information technology, including ROCS. In that role, Camacho had the ability and authority to access RMP's computer system, including ROCS, remotely.

In late August 2008, Camacho advised RMP that he was resigning his position in order to accept alternate employment. At the time his resignation became effective, Camacho was the leader of a project to build a web-based interface for ROCS that could be used by RMP's customers at their own facilities. At the time Camacho announced his intention to resign from RMP, the project was still several months from completion. Because Camacho had been the primary contact for vendors involved in the project, and a replacement for him had not yet been hired, RMP determined that it needed Camacho's continued involvement in order to complete the project on time. Consequently, on August 28, 2008, Camacho and RMP entered into a consulting agreement pursuant to which Camacho would continue to work as an independent contractor and would be paid an hourly rate for work performed supervising the completion of the project. After his resignation, Camacho continued to work on the project part-time, as an independent contractor, for six to eight weeks until the project was completed. During that time, Camacho had access, including remote access, to RMP's computer system, and specifically to the ROCS source code.

RMP alleges that as former employees of RMP, Camacho and the other employees who left RMP to go work for AllParts had an obligation not to divulge or disclose information gained in connection with their employment with RMP to any other person or company, but that Camacho and AllParts (through its employees) violated RMP's protectable interests in ROCS and caused injury to RMP through the use and disclosure of the ROCS application for their own business purposes and to compete unfairly with RMP.

RMP asserts, based upon these facts, that Camacho and AllParts violated the CFAA. Under Count I of the complaint, which purports to assert a cause of action under the CFAA, RMP alleges specifically that (1) RMP's computers and computer systems are "protected computers" for purposes of the CFAA (Verified Compl. ¶ 70); (2) Camacho intentionally accessed RMP's protected computer system "without authorization and/or in excess of authorized access, and thereby obtained information from [RMP's] protected computer system (*id.* ¶ 71); (3) "Camacho knowingly and with intent to defraud, accessed [RMP's] protected computer system, without authorization and/or in excess of authorized access" (*id.* ¶ 72); (4) Camacho thereby "furthered the intended fraud, obtained unauthorized use of [RMP's] protected computer systems, and obtained [RMP's] proprietary information, the value of such exceeding $5,000 in any one year period" (*id.* ¶ 73); (5) Camacho's wrongful actions were induced by, or performed with the knowledge and participation of, AllParts, and/or for AllParts' benefit, such that AllParts is “equally responsible for the wrongful conduct of Camacho” (*id.* ¶ 74); (6) through their intentional and unauthorized access to RMP’s computer system, Defendants caused RMP “damage and loss” (*id.* ¶ 75), and (7) such damage and loss

> exceeds $5,000 in value during any one year period, in that [RMP] has spent well in excess of $5,000 in investigating the wrongful acts committed by Camacho and AllParts and in seeking redress for those acts as well as in its efforts to locate and retain replacement employees. [RMP] has already suffered a reduction in business volume as compared to previous years. It is impossible at this time to quantify the additional damages to [RMP’s] business.

(*Id.* ¶ 76.)

The question posed by Defendants’ motions to dismiss is whether these allegations are sufficient to state a cause of action for violation of the CFAA.

III. LEGAL ANALYSIS AND DISCUSSION

A. The CFAA

The CFAA prohibits certain conduct involving unauthorized access to computers. *See* 18 U.S.C. § 1030(a)(1)–(a)(7). Although the CFAA is primarily a criminal statute, it also permits “[a]ny person who suffers damage or loss by reason of a violation of this section [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” *Id.* § 1030(g).

In the present case, RMP apparently seeks to assert that Defendants violated subsection (a)(2)(C) of 18 U.S.C. § 1030, which prohibits “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer”; subsection (a)(4), which prohibits “knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value”; and subsection (a)(5), which provides for liability on the part of any person who

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

18 U.S.C. § 1030(a)(5).[1]

Thus, for all civil claims under the CFAA, a plaintiff must show that the defendant's access to the protected computer was either "without authorization" or that it "exceed[ed] authorized access." Further, the scope of the CFAA is limited to civil claims premised upon "conduct involv[ing] 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g). The only subclause in the referenced subsection that is relevant to the present action requires the showing of "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). It is under this provision that RMP asserts its CFA claims.

Defendants seek dismissal of RMP's CFAA claims on the basis that RMP has not alleged that AllParts accessed RMP's computers at all, and has not alleged that Camacho's access was either without authorization or that in excess of his authorization as required in order to state a claim under the statute. Defendants also argue, in the alternative, that RMP has failed to allege facts suggesting it suffered "damage" or "loss," as those terms are defined by the CFAA, by any action taken by the Defendants. The Court finds both arguments to be meritorious, and either of them alone provides sufficient basis for dismissal of the CFAA claims.

B. RMP Has Not Alleged Facts Showing Camacho Lacked Authorization or Exceeded Authorization.

The Verified Complaint expressly alleges that Camacho had access, including remote access, to RMP's computer system and to the ROCS source code for the purpose of performing his job while he was still an employee, and for performing the tasks he undertook as an independent contractor after he formally resigned his employment. (Verified Compl. ¶¶ 47, 53.) While working for RMP, Camacho "created upgrades to the source code for ROCS" and was "responsible for the maintenance, modification and enhancement of ROCS"; "for integrating ROCS into [RMP's] computer system"; and "for maintaining and providing technical support for [RMP's] information technology, including ROCS." (Verified Compl. ¶¶ 47, 48.) In other words, it is clear from the allegations in the Verified Complaint that Camacho was authorized to access all parts of RMP's computer system and the ROCS application while he was either employed by RMP or working as an independent contractor. RMP does not allege that Camacho

[1] The term "protected computer" is defined by the Act to include any computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

continued to access its computer system after his authority expired, and it does not assert that any other person associated with AllParts ever accessed RMP's computer system. Rather, the crux of RMP's claims is that Camacho shared the information from RMP's computer system that he obtained while he had authorization to access and to obtain that information—in other words, that Camacho *used* the information he was authorized to obtain in a fashion that was adverse to RMP's interests and therefore beyond the bounds of his agency.

On the basis of these allegations, Defendants assert that this action must be dismissed because the CFAA only prohibits conduct that involves access without authorization or that exceeds authorization, and Camacho clearly had authorization to access all aspects of the ROCS application. RMP, on the other hand, asserts that by unlawfully breaching his duty of loyalty and agreement to maintain the confidentiality of RMP's trade secrets, Camacho exceeded his authority, regardless of the fact that he had the authorization to access the information in the first place.

There is, in fact, a split in legal authority as to whether the CFAA applies in a situation where an employee who has been granted access to his employer's computers, but uses that access for an improper purpose. The Sixth Circuit has not addressed the issue, but several district courts within this circuit have done so, including the Western District of Tennessee in a very thorough analysis. *Black & Decker (US), Inc. v. Smith*, 568 F. Supp. 2d 929 (W.D. Tenn. 2008). As the court there noted, both the Seventh and First Circuits, as well as several district courts, have found that an employee may exceed his authorization if he retrieves confidential or proprietary information from his employer's computer system that he is technically authorized to access, but then uses that information in a manner that is inconsistent with the employer's interests or in a manner that violates a contractual obligation. *Id.* at 933 (citing *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000)).[2] In *Citrin* and *Shurgard* in particular, the courts

[2] The *Black & Decker* court also referenced the opinion of the undersigned in *International Security Management Group, Inc., v. Sawyer*, No. 3:06cv0456, 2006 U.S. Dist. LEXIS 37059, at *58–*59 (M.D. Tenn. June 6, 2006), in which this Court adopted the holdings of *Explorica* and *Shurgard Storage* without analysis in ruling on a motion for preliminary injunction. Jurisdiction in that case was premised upon diversity, and the parties did not raise any specific arguments regarding the applicability of the CFAA to the activity alleged in the complaint in that case.

"relied on the rules of agency, finding that the authority of an agent terminates when he acquires adverse interests or is otherwise guilty of a serious breach of loyalty to the principal." *Black & Decker*, 568 F. Supp. 2d at 934 (citing *Citrin*, 440 F.3d at 420–21 (noting that the former employee's breach of loyalty terminated his agency relationship); *Shurgard*, 119 F. Supp. 2d at 1125 (same, citing Restatement (Second) of Agency § 112 (1958)). In other words, the analysis in those cases hinged on a finding that an employee oversteps whatever authority he is otherwise granted "the minute his intentions are adverse to those of his principal." *Id.*

Other courts, however, including the Ninth Circuit and numerous district courts, have rejected this rationale to hold that the CFAA targets the unauthorized procurement or alteration of information rather than its misuse. In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the Ninth Circuit first engaged in a plain-language reading of the statute, pursuant to which the court construed the term "without authorization" to mean "without permission." *Id.* at 1133. The court specifically rejected the agency theory of authorization espoused in *Citrin*, noting first that the CFAA was "primarily a criminal statute," and that, where a statute has both criminal and civil applications, it should be construed consistently in both contexts. Second, the court observed that it was "well established that 'ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.' " *Id.* (quoting *Rewis v. United States*, 401 U.S. 808, 812 (1971). Because the court found that *Citrin*'s interpretation of the statue "did not comport with the plain language" thereof, and because criminal statutes must be interpreted "to ensure that defendants are on notice as to which acts are criminal," the court held that

> a person uses a computer "without authorization" . . . when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

Id. at 1135. Based upon the same reasoning, the court also noted that the defendant did not "exceed authorization" where there was not dispute that he was entitled to obtain the documents at issue as part of his job. *Id.* at 1135 n.7. *Cf. Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (rejecting *Citrin* and *Shurgard* and holding that the plain language of the statute supports a narrower interpretation because (1) "without authorization" means without permission and (2) the CFAA's definition of "exceeds authorized access" contemplates a situation where " 'access [to a computer] is improper because the defendant accesses information to which he is not entitled,' " rather than misuses information that he is authorized to access) (quoting *Diamond Power Int'l v. Davidson*, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007)); *Brett Senior & Assocs., P.C. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377, at *4, (E.D. Pa. July 13, 2007) ("The common thread running through [cases like *Explorica*] is a focus on the employee's motive for accessing a computer and his or her intended use of the information obtained. As stated above, however, this interpretation reads section (a)(4) as if it said 'exceeds authorized use' instead of 'exceeds authorized access.' "); *Lockheed Martin Corp. v. Speed*, No. 6:05-cv-1580, 2006 WL 2683058, at *6 (M.D. Fla. Aug. 1, 2006) ("In this Court's view, the plain meaning brings clarity to the picture and illuminates the straightforward intention of Congress, *i.e.*, 'without authorization' means no access authorization and 'exceeds authorized access' means to go beyond the access permitted. While *Citrin* attempts to stretch 'without authorization' to cover those with access authorization (albeit those with adverse interests), Congress did not so stipulate.").

In *Black & Decker*, the Western District of Tennessee likewise rejected the *Citrin-Shurgard* line of cases and construed "without authorization" and "exceeds access" narrowly, using reasoning very similar to that of the Ninth Circuit in *LVRC Holding*:

> As with any question of statutory interpretation, [the Court] must first look to the language of the statute itself. If the language of the statute is unambiguous, courts need look no further. Only if the statute is inescapably ambiguous should a court look to other persuasive authority in an attempt to discern legislative meaning. Persuasive authority includes legislative history, policy rationales, other court decisions, the context in which the statute was passed, and other statutes. Because this is a criminal statute, even though it is being applied in a civil context, the Court must apply the rule of lenity, so that the statute is interpreted consistently. The rule of lenity requires that ambiguities [be] resolved in favor of the party accused of violating the law.
>
> As stated above, the statute defines the term "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). The Court agrees . . . that the plain meaning of "exceeds authorized access" is "to go beyond the access permitted." Likewise, while there is no definition for access "without authorization," the Court finds that its plain meaning is "no access authorization." The Defendant's alleged conduct clearly does not fall under these definitions, however, as he was permitted access to [Plaintiff's] network and any information on that network. The fact that he did not have permission to subsequently misuse the data he accessed by sharing it with any of his former employer's competitors is another matter that may be circumscribed by a different statute. Even if the [CFAA] were ambiguous on the subject of whether it applies to an insider who breaches his contractual obligations to his employer to keep certain information confidential, the rule of lenity would require that this ambiguity be resolved in favor of the Defendant.

Black & Decker, 568 F. Supp. 2d at 934–35 (most internal quotation marks and citations omitted). The court also went on to analyze the legislative history and found that it provided further support for the conclusion that Congress did not intend the CFAA to extend to situations where the access was technically authorized but the particular use of the information was not. *Id.* at 835–36 (focusing on the use of the terms “without authorization” and “exceeds authorization,” as well as the idea that “the legislative history supports the conclusion that Congress intended the CFAA to do ‘for computers what trespass and burglary laws did for real property’ (quoting Orin S. Kerr, Cybercrimes’ Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1617 (2003)); and noting that, although the scope of the statute had been broadened several times, the amendments related primarily to the penalties associated with violations but did not change the requirement that access be “without authorization” or “in excess of authorization).

Based upon its reading of the statute, the Western District ultimately concluded that the plaintiff in that case failed to state a civil claim under the CFAA, under circumstances basically indistinguishable from those presented here. As the Court stated:

> Because [the Defendant] had permission to access the information in question and doing so was within the scope of his duties, it cannot be successfully argued that his access constituted a trespass. Clearly, the Plaintiff objects not to [Defendant]'s accessing of the information, but to his later misuse thereof. Thus, while the Complaint includes claims that the Defendant breached both the Employee Access Agreement and the confidentiality agreements by allegedly disclosing [Plaintiff’s] trade secrets and proprietary information, the Court finds that no facts alleged indicate that [Defendant] exceeded the access he was granted by the Plaintiff or that he accessed the data without authorization.

Id. at 936. The *Black & Decker* court therefore dismissed the claims brought under subsections (a)(2), (a)(4), and (a)(5)(A) 18 U.S.C. § 1030.

The facts in the case before this Court compel the same result. The allegations in the Verified Complaint make it clear that Camacho was authorized to access all aspects of the ROCS application while he was engaged by RMP. RMP complains, not that Camacho went beyond his authorization to access information he was not entitled to see, but that he subsequently misused that information by sharing it with AllParts. RMP does not allege that AllParts itself, or any person other than Camacho, wrongfully accessed its computer system. The CFAA claims are subject to dismissal on the grounds that RMP has not alleged facts sufficient to establish an essential element of those claims, that is, that access to RMP’s computers was either without authorization or in excess of authority. The claims against AllParts must fail because RMP has not alleged that AllParts accessed its computers at all.

C. RMP Has Not Alleged "Loss" of the Type Covered by the CFAA.

Alternatively, Defendants assert that RMP's CFAA claims are subject to dismissal because RMP has not alleged that it suffered the type of "loss" for which the statute provides recovery.

Under the statute,

> the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Id. § 1030(e)(11).

An examination of the Verified Complaint demonstrates that RMP has not pleaded the sort of "loss" contemplated by the statute and has accordingly failed to state a claim under 18 U.S.C. § 1030(g). RMP alleges that AllParts has wrongfully been using its proprietary software platform since sometime in 2007, without RMP having any knowledge of that fact until recently. Obviously AllParts' use of the program did not impair RMP's ability to use it. RMP learned in August 2009 that AllParts' had updated its system in July 2009, using information obtained by Camacho while he was working for RMP. Camacho had stopped working for RMP nearly a year previously. Obviously, Camacho's copying or use of information did not actually damage RMP's system or impair RMP's ability to use it. The loss at issue is the misappropriation of RMP's confidential, trade-secret information, which has damaged RMP's business interests. RMP alleges that it "spent well in excess of $5,000 in investigating the wrongful acts committed by Camacho and AllParts and in seeking redress for those acts as well as in its efforts to locate and retain replacement employees. [RMP] has already suffered a reduction in business volume as compared to previous years." (Doc. No. 1, Verified Compl. ¶ 76.)

Clearly, RMP has not alleged that AllParts caused any physical damage to its computer data, system or programs in the sense of an impairment to their integrity or availability, and RMP does not seriously argue to the contrary. RMP does argue, however, that it has adequately pleaded that it suffered "losses" as the term is defined by the CFAA. The Court finds, however, that the only reasonable inference to be drawn from the Complaint is that RMP has suffered lost revenue and damages associated with Camacho's misappropriation of its trade-secret information. Under the statute, lost revenue is only recoverable if it was incurred because of an "interruption in service," 18 U.S.C. § 1030(g), but RMP has not alleged any disruption in its service. Moreover, the "investigation" of AllParts' alleged wrongful acts (*i.e.*, the misappropriation of confidential information), as well as the costs incurred by RMP in its efforts to seek redress for those acts and to retain new employees are likewise not the type of loss that are covered by the statute. Rather, these are the types of injuries associated with any trade-secrets misappropriation action and are certainly not related to analyzing or restoring the system to its previous condition or to any interruption in service. *Cf. Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 772 (N.D. Ohio 2008) ("The CFAA does not contemplate consequential damages . . . that are unrelated to harm to the computer itself."); *L-3 Commc'ns. Westwood Corp. v. Robicharux*, No. 06-0279, 2007 WL 756528, at *4 (E.D. La. Mar. 8, 2007) ("Losses under CFAA are compensable when they result from damage to a computer system or the inoperability of the accessed system."); *Nexans Wires, S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004) ("The meaning of 'Loss' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer or a cost incurred because the computer's service was interrupted."), *aff'd*, 166 Fed. Appx. 559 (2d Cir. 2006); *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009) ("Purely economic harm unrelated to the computer systems is not covered by this definition."); *Cheney v. IPD Analytics, LLC*, No. 08-23188-CIV, 2009 WL 1298405, *7 (S.D. Fla. Apr. 16, 2009) (finding defendants failed to state a claim on their counterclaim under the CFAA in part because a "[p]lain reading of the definition of 'loss' under the statute suggests that any 'loss' must be related to interruption of service," and "the claim fails to allege that Analytics suffered any 'interruption of service' "); *ES&H, Inc. v. Allied Safety Consultants, Inc.*, No. 3:08-cv-323, 2009 WL 2996340, at *4 (E.D. Tenn. Sept. 16, 2009) (same, collecting cases).

This Court is not persuaded by the contrary authority upon which RMP relies in its response in opposition to Defendants' motions. Some of the cases cited by the plaintiff do not actually support its position.[3] The others for the most part adopt the "broad" view of the terms authorization and "exceeds

[3] *See, e.g.*, *Bloomington-Normal Seating Co. v. Albritton*, 2009 WL 1329123 (C.D. Ill. May 13, 2009) (where the access in question was clearly in excess of authorization, holding that "loss" under the statute "is limited to costs that are directly associated with, or with addressing, an unauthorized computer-access event," and also holding that a plaintiff need not establish *both* damages *and* loss under the statute); *NCMIC Fin. Corp. v. Artino*, 638 F. Supp. 2d 1042 (S.D. Iowa 2009) (where an actual security breach was alleged to have occurred, construing "loss" to cover costs associated with "responding to a security breach"); *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975 (N.D. Cal. 2008) (involving an actual hacking of plaintiff's computer system by plaintiff's competitor company, resulting in losses associated with trying to ascertain how the security breach occurred and by whom); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008) (dismissing complaint after adopting the "narrow" construction of the term "exceeds authorization").

authorization" which, as discussed above, this Court rejects.[4] Those courts adopting the broad view of those terms have generally also adopted a broad view of the definition of the term "loss," which this Court likewise declines to follow.

In sum, RMP's failure to allege facts reasonably giving rise to an inference that it suffered the type of "loss" recognized by the CFAA provides an alternative basis for dismissal of the CFAA claims. On this ground as well, Defendants' motion is meritorious.

IV. CONCLUSION

To state a civil claim under the CFAA, a plaintiff must allege, as an element of the cause of action, first that the access to the protected computer was either unauthorized or in excess of the authorization granted, and that as a result of that unauthorized access it suffered "loss" as that term is defined by the statute. Plaintiff RMP simply has not alleged in the Verified Complaint that the access to its computer system by Camacho exceeded his authorization, or that RMP suffered the type of loss covered by the statute, even construing the allegations in the light most favorable to the plaintiff and drawing all inferences in its favor. As a result, the claims under the CFAA must be dismissed. Having concluded that dismissal of the federal claims asserted in the complaint is warranted, the Court will decline to exercise supplemental jurisdiction over the state-law claims and will dismiss those without prejudice, pursuant to the discretion granted by 28 U.S.C. § 1367(c)(3).

An appropriate Order granting Defendants' motions and dismissing this action will enter separately.

Thomas A. Wiseman, Jr.
Thomas A. Wiseman, Jr.
Senior U.S. District Judge

[4] . *See, e.g.*, *Ervin & Smith Adver. & Pub. Relations, Inc. v. Ervin*, No. 8:08CV459, 2009 WL 249998, at *7–*8 (D. Neb. Feb. 3, 2009) (interpreting "authorization" broadly, following *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006), and *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 (1st Cir. 2001), and likewise interpreting "loss" broadly to cover lost business profits); *CoStar Realty Information, Inc. v. Field*, 612 F. Supp. 2d 660 (D. Md. 2009) (in a case involving clearly unauthorized access, concluding that lost revenue constituted "loss" under the statute); *Hudson Global Resources Holdings, Inc. v. Hill*, No. 02:07cv132, 2007 WL 707353, at*2–*3 (W.D. Pa. March 2, 2007) (adopting the reasoning of other "broad-view" cases without substantive analysis).